UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/014,763	12/11/2001	Juan A. Garay	8-32	6594

7590 07/13/2006

Ryan, Mason & Lewis, LLP
90 Forest Avenue
Locust Valley, NY 11560

EXAMINER
LEMMA, SAMSON B

ART UNIT	PAPER NUMBER
2132	

DATE MAILED: 07/13/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

BEFORE THE BOARD OF PATENT APPEALS
AND INTERFERENCES

Application Number:10/014,763
Filing Date: December 11, 2001
Appellant(s): GARAY ET AL.

Michael L. Wise
For Appellant

EXAMINER'S ANSWER

This is in response to the appeal brief filed on April 24,2006 appealing from the Office action mailed on November 23,2005, finally rejecting claims 1-25.

(1) Real Party in Interest

A statement identifying by name the real party in interest is contained in the brief.

2) Related Appeals and Interferences

The examiner is not aware of any related appeals, interferences, or judicial proceedings which will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

(3) Status of Claims

The statement of the status of claims contained in the brief is correct, except for claims 4-8.

The Examiner would like to note that although on pages 6-7 of the office action dated November 23, 2005, it was indicated that claims 2-8 was rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. Appellant, however, on page 3 of his appeal brief under the title, "**Grounds of Rejection To Be Reviewed on Appeal**", presented as if only claims 2-3 were rejected under 35 U.S.C. 112 without mentioning the dependent claims 4-8.

Therefore, a correct statement of the status of the claims follows below:

- **Claims 2-8** stand rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

- **Claims 1-7,9-10,17 and 19-25** stand rejected under 35 U.S.C. 102 as being anticipated by **Aura** (U.S. Patent No 6,711,400)
- **Claims 8,11-16 and 18** stands rejected under 35 U.S.C. 103 as being unpatentable over **Aura**(U.S. Patent No 6,711,400) **in view of Micali**(U.S. Patent No 5,016,274).

(4) Status of Amendments After Final

The appellant's statement of the status of amendments after final rejection contained in the brief is correct.

(5) Summary of Claimed Subject Matter

The summary of claimed subject matter contained in the brief is correct.

(6) Grounds of Rejection to be Reviewed on Appeal

The appellant's statement of the grounds of rejection to be reviewed on appeal is correct however with respect to dependent **claims 4-8**, Appellant presented as if only claims 2-3 were rejected under 35 U.S.C. 112 without mentioning the dependent claims 4-8.

Nevertheless, Examiner asserts that on page 7 of the final office action dated November 23, 2005, it was indicated that claims 4-8 were also rejected under under 35 U.S.C. 112 since they depend on rejected claims 2 and 3, and include all the limitations of the respective claim, thereby rendering those dependent claims indefinite. Therefore claims 2-8 stand rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

(7) Claims Appendix

The copy of the appealed claims contained in the Appendix to the brief is correct.

(8) Evidence Relied Upon

6,711,400	**Aura**	03-2004
5,016,274	**Micali**	05-1991

(9) Grounds of Rejection

The following ground(s) of rejection are applicable to the appealed claims:

Claim Rejections - 35 USC § 112

1. **Claim 2** is rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. Claim 2 recite the limitation "**having a computational efficiency compatible with computational resources of the user device**". This term is not only vague but also not clear. Examiner would point out that Appellant used relative terms in the specification for defining/explaining the computational efficiency (see page 1, lines 24-26 & page 7, lines 3-8). Terms like, "fast", "shorter amount of time", "less computational complexity" are used in the specification and such terms are relative terms which need to be some how quantified, otherwise it would not be clear for one of ordinary skill in the art to determine with out ambiguity

the extent/degree of how fast/slow/less/short the computational efficiency should be in order to be compatible with computational resources of the user device.

The claim has to be rewritten so that there would not be any ambiguity. For the purpose of examination the limitation is taken out from the respective claim.

2. **Claim 3** is rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. Claim 3 recite the limitation "...**having a computational efficiency lower than that of the first digital signature protocol.** " This term is not only vague but also not clear. Examiner would point out that Appellant used relative terms in the specification for defining/explaining the computational efficiency (see page 1, lines 24-26 & page 7, lines 3-8). Terms like, **"fast", "shorter amount of time", "less computational complexity"** are used in the specification and such terms are relative terms which need some how be quantified, otherwise it would not be clear for one of ordinary skill in the art to determine with out ambiguity the extent/degree of how fast/slow/less/short the computational efficiency should be in order to be compare it with digital signature protocol. Besides, the term "lower" used in the claim limitation is also a relative term. For the purpose of examination such limitation is taken out from the respective claim. The claim has to be rewritten so that there would not be any ambiguity.

3. **Claims 4-8** depend from rejected claim 2 and 3, and include all the limitations of the respective claim, thereby rendering those dependent claims indefinite.

Claim Rejections - 35 USC § 102

4. **Claims 1-7,9-10,17, 19-25** are rejected under 35 U.S.C. 102(e) as being anticipated by **Aura**. (hereinafter referred to as **Aura**) (U.S. Patent No. 6,711,400 B1).

5. **As per claim 1 and 22-25**

Aura discloses a method for use in generating digital signatures in an information processing system, the system including at least a user device, an intermediary device and a verifier, the method comprising the steps of:

- **Generating in the user device a first digital signature**; [Figure 4, reference "405" and ref. Num "SRES1";page 10, lines 1-3**)** (As disclosed on page 10, lines 1-3 and shown on figure 4, ref. Num "405", first digital signature "SRES1" is generated)

- **Sending the first digital signature to the verifier;** [figure 4, ref. Num "406"; page 10, lines 1-3](As discloses on page 10, lines 1-3 and shown on figure "406" and "405"; the first digital signature SRES1 is sent to the VPLMN which is met the verifier.)

- **Wherein the verifier sends the first digital signature to the intermediary device,** [figure 4, ref. Num "407" and ref. Num "SRES1" and page 10, line 6,] (the verifier which is met the VPLMN shown on figure 4, ref. Num "406" sends a first digital signature **"SRES1"** to the intermediary device which is met the "mobile station" shown on figure 4, ref. Num "407") and

- **The intermediary device checks that the first digital signature is a valid digital signature for the user device** [figure 4, ref. Num "408"; page 10, lines 17-20](Aura on page on page 10, lines 17-20 discloses that the same mobile station which is met to be intermediary device checks the validity of the first digital signature by comparing the first digital signature SRES1 to the values SRES1' it has generated itself**)** **and .**

- **If the first digital signature is valid [figure 4, ref. Num "408", "Yes"] generates a second digital signature** [figure 4, ref. Num "407 & 408" and "SRES2"] **which is returned to the verifier** (figure 4, ref. Num "SRES2", "409"**) as a signature generated by the user device** [Figure 4, ref. "SRES2" and Num "408"]. (Aura on page on page 10, lines 17-20 discloses that the same mobile station which is met to be intermediary device checks the validity of the first digital signature by comparing the first digital signature SRES1 to the values SRES1' it has generated itself. Aura on page 20-21, further discloses the fact that after successful identification or if the first digital signature is found valid, the same mobile station sends the generated SRES2/second digital signature to the same/said verifier/ network VPLMN.)

6. **As per claim 2, Aura discloses** a method for use in generating digital signatures in an information processing system as applied to claim 1 above. Furthermore Aura discloses the method wherein the first digital signature is generated using a first secret key. [See figure 4, ref. Num "405" and secret Key "Ki" and "SRES1"]

7. **As per claim 3, Aura discloses** a method for use in generating digital signatures in an information processing system as applied to claim 1 above. Furthermore Aura discloses the method wherein the second digital signature is generated using a second secret key [See figure 4, ref. Num "407" and secret key "KI" and "SRES2"]

8. **As per claim 4 and 5, Aura discloses** a method for use in generating digital signatures in an information processing system as applied to claim 1 above. Furthermore Aura discloses the method wherein an agreement relating to corresponding public keys of the first and second digital signature protocols is signed by both the user device and the intermediary device and the resulting twice-signed agreement is stored by both the user device and the intermediary device. [Figure 4]

9. **As per claim 6, Aura discloses** a method for use in generating digital signatures in an information processing system as applied to claim 1 above. Furthermore Aura discloses the method wherein **the first digital signature comprises a signature s1 on a message m,** [figure 4, ref. 405 and "SRES1"] the **signature s1 being generated using a secret key s'** [figure 4, ref. Num "405" and "Ki"] **associated with the user device**. [figure 4]

10. **As per claim 7, Aura discloses** a method for use in generating digital signatures in an information processing system as applied to claim 1 above. Furthermore **Aura discloses the method wherein the first digital signature comprises a signature s1 on h(m),** [figure 4, ref. Num "405" See H1] **where m is a message and h is a hash function, the signature s1 being generated using a secret key s'** [figure 4, ref. Num "405" and "Ki"] **associated with the user device.** [figure 4]

11. **As per claim 9, Aura discloses** a method for use in generating digital signatures in an information processing system as applied to claim 1 above. Furthermore **Aura discloses the method wherein the second digital signature comprises a signature s2 on a message m,** [figure 4, ref. Num "SRES2"] **the signature s2 being generated using a secret key s** [figure 4, ref. Num "407" See KI] of **associated with the user device. [figure 4]**

12. **As per claim 10, Aura discloses** a method for use in generating digital signatures in an information processing system as applied to claim 1 above. Furthermore **Aura discloses the method wherein the second digital signature comprises a signature s2** [figure 4, ref. Num "407", "SRES2"] **on h(m), where m is a message and h is a hash function,** [Figure 4, ref. Num "407" and H2] **the signature s2 being generated using a secret key s** [figure 4, ref. Num "407" See KI] of **associated with the user device. [figure 4]**

13. **As per claim 17, Aura discloses** a method for use in generating digital signatures in an information processing system as applied to claim 1 above. Furthermore **Aura discloses the method wherein** the intermediary device is configured to wait a predetermined delay period

between checking that the first digital signature is a valid signature and generating the second digital signature which is returned to the verifier. [Figure 4, ref. Num "408"]

14. **As per claim 19-21, Aura discloses** a method for use in generating digital signatures in an information processing system as applied to claim 1 above. Furthermore **Aura discloses the method wherein** the user device comprises a mobile telephone.[figure 1]

Claim Rejections - 35 USC § 103

15. **Claims 8,11-16,18** are rejected under 35 U.S.C. 103(a) as being unpatentable **Aura**. (hereinafter referred to as **Aura**) (U.S. Patent No. 6,711,400 B1).
in view of **Micali et al**, (hereinafter referred to as **Micali**) (U.S. Patent No. 5,016,274)

16. **As per claim 8,11-16 and 18 Aura** discloses verifier upon receipt of the first digital signature checks that the first digital signature is a valid digital signature using [Figure 4, ref. Num "409"]

Aura does not explicitly disclose that verifier upon receipt of the first digital signature checks that the first digital signature is a valid digital signature **using a first public key corresponding to the first secret key.**

However, in the same field of endeavor, **Micali** discloses that verifier upon receipt of the first digital signature checks that the first digital signature is a valid digital signature **using a first public key corresponding to the first secret key. [Figure 1, ref. Num "34"]**

It would have been obvious to one having ordinary skill in the art, at the time
the invention was made, to combine the features of verification digitat signature
using the public key as per teaching of Micali in to the method verification as

taught by **Aura**, in order to enhances the security and efficiency of known signature schemes.[See Micali Column 1, lines 7-9]

(10) Response to Argument

Appellant's argument filed with the Appeal brief, on April 24, 2006 have been fully considered but they are not persuasive.

Referring to the dependent claim 2, Rejections - 35 USC § 112, *Appellant argued that the scope of the limitation, "**having a computational efficiency compatible with computational resources of the user device**" would be clear to one skilled in the art in light of ordinary and customary meanings of the words and their usage in the specification. Aspects of computational efficiency and computational resources are described in the specification at, for example, p. 1, lines 12-26 and p.7, lines 3-8.*

Examiner disagrees with the above argument and would point out that on page 1, lines 12-15, the following has been recited. "The portable communication devices such as mobile telephones, personal digital assistants (PDAs) and "wearable" computers generally have **limited computational resources in terms of one or more factors such as memory, processing power, communication bandwidth and network connection time.** Such devices are therefore referred to herein as lightweight devices." Furthermore, the specification on page 1, lines 24-26, further recites the following. "While there are conventional signature protocols, such as Merkle and Lamport signatures, that are well suited for lightweight device applications, these signatures are generally incompatible with existing and proposed public-key infrastructures (PKIs)." Likewise on page 7, lines 3-8, the specification recites the following.

"The user then in step 302 creates a second key pair (s', p') that is suitable for **"fast"** generation of signatures. More particularly, this second key pair may be a key pair associated with a conventional computationally-efficient signature technique, such as Merkle and Lamport signatures, signature coupons, etc., that is suitable for implementation on a lightweight device. **Such techniques are referred to as "fast" in that they can be performed with less computational complexity, and therefore in a shorter amount of time, than other signature techniques."**

As shown above, Examiner would point out that Appellant used relative terms in the specification for defining/explaining the computational efficiency. Terms like, "fast", "shorter amount of time", "less computational complexity" are used in the specification and such terms are relative terms which need to be some how quantified, otherwise it would not be clear for one of ordinary skill in the art to determine with out ambiguity the extent/degree of how fast/slow/less/short the computational efficiency should be in order to be compatible with computational resources of the user device. The office understood the difficulty of quantifying such terms; the point however is, if such terms are not determined and assigned some values, one of ordinary skill in the art would not be able to understand the limitation presented in the dependent claim 2. Therefore the Rejection under 35 USC § 112 given for dependent claim 2 is proper and is maintained by the office.

Referring to the dependent claim 3, Rejections - 35 USC § 112, *Appellant argued that the scope of the limitation, "**having a computational efficiency lower than that of the first digital signature protocol**" would be clear to one skilled in the art in light of ordinary and customary meanings of the words and their usage in the specification. Aspects of computational efficiency and computational resources are described in the specification at, for example, p. 1, lines 12-26 and p.7, lines 3-8.*

Examiner disagrees with the above argument

As indicated above, Examiner would point out that Appellant used relative terms in the specification for defining/explaining the computational efficiency. Terms like, **"fast", "shorter amount of time", "less computational complexity"** are used in the specification and such terms are relative terms which need some how be quantified, otherwise it would not be clear for one of ordinary skill in the art to determine with out ambiguity the extent/degree of how fast/slow/less/short the computational efficiency should be in order to compare it with digital signature protocol. Besides, the term "lower" used in the claim limitation is also a relative term. The office understood the difficulty of quantifying such terms; the point however is, if such terms are not determined and assigned some values, one of ordinary skill in the art would not be able to determine "how low" the computational efficiency should be when it is compared with the first digital signature protocol as it is presented in the dependent claim 3. Therefore the Rejection under 35 USC § 112, given for claim 3 is proper and is maintained by the office.

Referring to the independent claim 1, Rejections - 35 USC § 102 (e), **Appellant argued** that the interpretation of the "user device" in the claim limitation as "Authentication center" in the reference and the "intermediary device" in the claim limitation as "mobile station" in the reference is wrong, therefore Appellant argued that each and every limitation of the claim is not anticipated by the reference on the record, namely Aura.

Appellant wrote the following in support of his argument.

"In formulating the §102(e) rejection of this claim, the Examiner argues that each and every claimed element is anticipated by Aura. More specifically, the Examiner argues that the authentication centre" in Aura's FIG. 4 (labeled "AUC" in the figure) describes the "user device" in claim 1 (Final Office Action, #10, first bullet point). What is more, the Examiner argues that the mobile station Aura's FIG. 4 (labeled "MS" in the figure) describes the "intermediary device" in the claim (Final Office Action, #10, fourth and fifth bullet points). Appellants respectfully submit that both assertions are untenable."

"In Aura, an authentication centre is connected to a home location register and is a fixed element in a network (Aura, FIG. 1 and col. 1, lines 38-59). The authentication centre performs processing tasks related to authenticating the identity of the network (Aura, col. 5, lines 21-51). In contrast, the user device in claim 1, as the name clearly indicates, is a device that is operated by a user. Embodiments of the user device may comprise, for example, a mobile telephone, PDA, desktop or portable computer, or television set-top box (**Specitication, p. 5, lines 11- 16**). As a result, it is clear that Aura's authentication centre does not describe the user device in claim 1. Aura's mobile station, moreover, comprises mobile equipment and a subscriber identity module (Aura, col. 1 , line 66 to col. 2, line 3). A mobile station is operated by a mobile subscriber (i.e., user) (Aura, col. 1, lines 49-59). The intermediary device in claim 1, in contrast, is operative to check that a first signature generated by a user device is valid and to generate a second digital signature which is a returned to the verifier as a signature generated by the user device. Again, it is clear that Aura's mobile station does not describe the intermediary device in claim 1. Consequently, Aura fails to describe each and every element of claim 1."

Examiner disagrees with this argument.

First of all, Examiner would point out that the interpretation made by the office is correct and meets the limitation of the claim since it corresponds to the definition of "user device" provided in the Appellant specification.

The limitation "user device" is defined in the Appellant specification on page 5, lines 11-16 as "a mobile telephone or PDA, or a device which may alternatively be implemented as a desktop or portable personal computer, a wearable computer, a television set-top box o**r any other type of device capable of transmitting or receiving information."**

Therefore the authentication center as shown on figure 4, not only capable of transmitting or receiving information but also meets the limitation of a computer. Therefore a user device which can be any type of device/computer capable of transmitting or receiving information is undoubtedly anticipated by the "Authentication center".

The other argument made by the Appellant about the limitation of the intermediary device, which is interpreted by the office as mobile station, is also wrong for the following reason.

Appellant wrote the following, "Aura's mobile station, moreover, comprises mobile equipment and a subscriber identity module (Aura, col. 1 , line 66 to col. 2, line 3). A mobile station is operated by a mobile subscriber (i.e., user) (Aura, col. 1, lines 49-59). The intermediary device in claim 1, in contrast, is operative to check that a first signature generated by a user device is valid and to generate a second digital signature which is a returned to the verifier as a signature generated by the user device. Again, it is clear that Aura's mobile station does not describe the intermediary device in claim 1. Consequently, Aura fails to describe each and every element of claim 1."

However, the examiner would show that the mobile station shown on figure 4, ref. Num "407" and "408" not only checks that a first signature generated by a user device is valid [figure 4, ref. Num "408"] but also generates a second digital signature [SRES2] which is a returned to the verifier [figure 4, ref. Num "409", "406"].

Therefore examiner asserts that the rejection is valid. Furthermore for purpose of clarifying the rejection, Examiner show how each and every limitation described in the independent claims 1, 22-25 **is anticipated/disclosed by Aura as follows.**

Aura discloses

- **Generating in the user device a first digital signature**; [Figure 4, reference "405" and ref. Num "SRES1";page 10, lines 1-3) (As disclosed on page 10, lines 1-3 and shown on figure 4, ref. Num "405", first digital signature "SRES1" is generated)

- **Sending the first digital signature to the verifier;** [figure 4, ref. Num "406", "SRES1"; page 10, lines 1-3](As discloses on page 10, lines 1-3 and shown on figure "406" and "405"; the first digital signature SRES1 is sent to the VPLMN which is met the verifier.)

- **Wherein the verifier sends the first digital signature to the intermediary device,** [figure 4, ref. Num "407" and ref. Num "SRES1" and page 10, line 6,] (the verifier which is met the VPLMN shown on figure 4, ref. Num "406" sends a first digital signature **"SRES1"** to the intermediary device which is met the "mobile station" shown on figure 4, ref. Num "407") and

- **The intermediary device checks that the first digital signature is a valid digital signature for the user device** [figure 4, ref. Num "408"; page 10, lines 17-20](Aura on page on page 10, lines 17-20 discloses that the same mobile station which is met to be intermediary device checks the validity of the first digital signature by comparing the first digital signature SRES1 to the values SRES1' it has generated itself**)** **and .**

- **If the first digital signature is valid [figure 4, ref. Num "408", "Yes"] generates a second digital signature** [figure 4, ref. Num "407 & 408", "SRES2"**] which is returned to the verifier (**figure 4, ref. Num "SRES2", "409"**) as a signature generated by the user device [**Figure 4, ref. "SRES2" and Num "408"**]**. (Aura on page on page 10, lines 17-20 discloses that the same mobile station which is met to be intermediary device checks the validity of the first digital signature by comparing the first digital signature SRES1 to the values SRES1' it has generated itself. Aura on page 20-21, further discloses the fact that after successful identification or if the first digital signature is found valid, the same mobile station sends the generated SRES2/second digital signature to the same/said verifier/ network VPLMN.)

The rest of Appellant argument is regarding the dependent claims, that are depending on to the respective independent claims 1, 22-25.

Appellant argued that since the independent claims are allowable therefore all the claims dependent thereon are also in condition for allowance for the same reasons argued for the independent claim.

In response to the above argument by the Appellant, **the examiner replies** that the respective dependent claims stands or fall with the independent claims.

(11) Related Proceeding(s) Appendix

No decision rendered by a court or the Board is identified by the examiner in the Related Appeals and Interferences section of this examiner's answer.

For the above reasons, it is believed that the rejections should be sustained.

Respectfully submitted,

Samson Lemma
S.L.
07/01/2006

Conferees:

Gilberto Barron

Benjamin Lanier

GILBERTO BARRON JR.
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100